victory established Big Daddy as a major player in professional drag racing.

With wife Pat and daughters Gay Lyn and Donna by his side, Garlits dominated the sport for nearly three decades, developing innovative technology, setting speed records and enduring several major crashes.

In the early 1970's, Garlits once again made history. It wasn't another speed record, but rather the design of Swamp Rat 14, the world's first successful rear engined dragster.

''I think that's my legacy, I really do,'' Garlits explained. ''I had so much opposition, everybody was against it. I took the car to Long Beach and the promoter didn't want me to run it. He told me every rear-engined car that ever went down his track crashed and he didn't want Don Garlits getting killed at his race track.''

The car went on to carry Big Daddy to another major championship and the rear-engine concept became the standard of the Top Fuel category.

Garlits achieved another of his personal goals in 1984, when he and his family opened the Museum of Drag Racing adjacent to his Marion County home. The sprawling complex on County Road 484 has grown to include an impressive display of nearly 17 race cars in addition to a collection of 70 classic and antique cars.

The complex also includes a race garage where Garlits is painstakingly building the newest and fastest Swamp Rat. He will race in next February at the NHRA Winternationals in Pomona, the site of his first major win.

''At the moment of launch, the motor will deliver 8,000 horsepower—roughly a thousand horsepower per cylinder,'' Garlits explained. ''It's really amazing, considering Swamp Rat One needed all eight cylinders to produce 750 horsepower.''

He expects the new state-of-the-art top fuel dragster to reach speeds in excess of 330 miles per hour in about four and a half seconds. Despite the high speeds, Garlits feels this Swamp Rat is the safest ever built.

''The first few generations of cars were just big motors, seats and fuel tanks strapped onto a couple of chassis rails. They didn't have near the safety technology used in today's cars,'' he explained.

Garlits believes new technology will continue to move forward and future race cars will be much faster and much safer than the current models.

''We are being limited by new rules, not by technology and I agree with that,'' he said. ''Most current drag strips are too short and too narrow to accommodate the kind of speeds that technology is capable of producing. We're just at the tip of the iceberg in terms of what is technologically possible.''

Like a scene out of one of the Back to the Future movies, a slight smile crossed Big Daddy's face as he talked about the future. Because he intends to be a part of it. That's how racers think.

PERSONAL EXPLANATION

HON. LUIS V. GUTIERREZ

OF ILLINOIS

IN THE HOUSE OF REPRESENTATIVES

Friday, November 16, 2001

Mr. GUTIERREZ. Mr. Speaker, I was unavoidably absent from this chamber when roll call vote 422 was taken. I want the record to show that had I been present in this chamber I would have voted ''nay'' on this rollcall vote.

INTRODUCTION OF THE COMPUTER SECURITY ENHANCEMENT AND RESEARCH ACT OF 2001

HON. BRIAN BAIRD

OF WASHINGTON

IN THE HOUSE OF REPRESENTATIVES

Friday, November 16, 2001

Mr. BAIRD. Mr. Speaker, today I am introducing the Computer Security Enhancement and Research Act of 2001. This legislation will address long-term needs in securing the nation's information infrastructure as well as strengthening the security of the non-classified computer systems of federal agencies. The bill establishes a research and development program on computer and network security at the National Institute of Standards and Technology. It also strengthens the Institute's existing responsibilities in developing best computer security practices and standards and in assisting federal agencies to implement effective computer and network security.

Because of September 11th, attention is focused in an unprecedented way on increasing our security against terrorism. Our concerns include protecting critical national infrastructures. Today, security has to mean more than locking doors or guarding buildings and installing metal detectors. In addition to physical security, virtual systems that are vital to the Nation's economy must be protected. Telecommunications and computer technologies are vulnerable to attack from far away by enemies who can remain anonymous, hidden in the vast maze of the Internet. Examples of systems that rely on computer networks include the electric power grid, rail networks, and financial transaction networks. Just as enemies are achieving a sophistication to use the most complex weapons against us, our vital computer networks have become more interconnected and more accessible via the Internet.

The vulnerability of the Internet to computer viruses, denial of service attacks, and defaced web sites is well known. These widely reported events have increased in frequency over time. These attacks disrupt business and government activities sometimes resulting in significant recovery costs. While no catastrophic cyber attack has occurred thus far, Richard Clarke, the President's new cyber-terrorism czar, has said that the government must make cybersecurity a priority or face the possibility of a ''digital Pearl Harbor''.

While potentially vulnerable computer systems are largely owned and operated by the private sector, the government has an important role in supporting the research and development activities that will provide the tools for protecting information systems. An essential component for ensuring improved information security is a vigorous and creative basic research effort focused on the security of networked information systems. Unfortunately, witnesses at a recent Science Committee hearing indicated that current R&D efforts fall far short of what's required.

Witnesses at the hearing noted the anemic level of funding for research on computer and network security. This lack of funding has resulted in the lack of a critical mass of researchers in this field and a focus on safe, incremental research projects. The witnesses advocated increased and sustained research funding from a federal agency assigned the role to support such research on a long-term basis. To date, Federal support for computer security research has been directed as defense and intelligence needs. While this work on encryption and defense systems security protocols is absolutely vital, very little has been done on the civilian side of communications security.

The bill I'm introducing explicitly addresses this gap in Federal support for computer security. My bill charges the National Institute of Standards and Technology (NIST) with implementing a substantial program of research support based at institutions of higher education designed to improve the security of networked information systems. This research program is authorized for a 10-year period, growing from $25 million in the 1st year to $85 million by the 5th year. Although awards are to universities, the research projects may involve collaborations with for-profit companies that develop information security products.

The bill establishes a flexible management approach for the research program. It is based upon a management style that has been used effectively by the Defense Advanced Research Projects Agency to spur advances in high technology fields. Specifically, management of the research program will rely on program managers who are both knowledgeable about computer security issues and needs and familiar with the research community. These program managers will be responsible for identifying and nurturing talented researchers and for generating innovative research proposals. Although program managers will have considerable freedom in managing their individual research portfolios, each will be reviewed periodically by NIST senior managers and by outside computer security experts. To ensure its relevance and continued need, the overall research program will be reviewed in its 5th year for scientific merit and relevance by the National Academy of Sciences.

An expanded university-based research program will train new graduate students and post-doctoral research assistants, as well as attracting seasoned researchers to the field. The result will be a larger and more vibrant basic research enterprise in computer-related security fields. A separate set of awards will be available to support post-doctoral research fellowships and senior research fellowships both at universities and at NIST. The bill also increases support for on-going, in-house computer security research at NIST.

The Computer Security Enhancement and Research Act of 2001 builds on the long experience of NIST in developing computer security standards and practices by placing new responsibilities on the agency for building up the nation's basic research enterprise in information security. By enlarging and strengthening the research enterprise we can generate the ideas and approaches needed to provide for future cyber security in an insecure world.

HARRY & IKE, THE PARTNERSHIP THAT REMADE THE POSTWAR WORLD—A HISTORY LESSON FOR ALL TO ENJOY

HON. WILLIAM O. LIPINSKI

OF ILLINOIS

IN THE HOUSE OF REPRESENTATIVES

Friday, November 16, 2001

Mr. LIPINSKI. Mr. Speaker, I rise tonight to recommend a new book by Chicago Sun